WHAT IS CLAIMED IS:

1. An article of manufacture comprising a computer readable medium on which server emulation software is stored and from which Interactive Media Site (IMS) software can be accessed by a local host device, wherein the computer readable medium comprises:

at least one virtual store from which a consumer may obtain at least one of a product and a service; and

financial card information for providing payment for the at least one of the product and the service obtained by the consumer.

2. The article of manufacture recited in claim 1, wherein the at least one virtual store comprises at least one virtual catalog of products that the consumer may order.

3. The article of manufacture recited in claim 1, wherein the financial card information comprises at least one of an encrypted credit card number and an encrypted debit card number.

4. The article of manufacture recited in claim 1, wherein the financial card information is embedded on the computer readable medium using an application program interface associated with the server emulation software.

5. The article of manufacture recited in claim 1, wherein the financial card information is automatically loaded into a memory device of the host device when the computer readable medium is accessed.

6. The article of manufacture recited in claim 5, wherein the memory device is a random access memory device.

7. The article of manufacture recited in claim 5, wherein the memory device is at least one of flushed and overwritten when the consumer completes a transaction.

8. The article of manufacture recited in claim 1, wherein the financial card information is relegated to first in first out access in the host device when the computer readable medium is accessed such that a port conveying the financial card information is only opened for a short period of time.

9. The article of manufacture recited in claim 1, wherein the financial card information is password protected.

10. The article of manufacture recited in claim 9, wherein the computer readable medium further comprises at least one of a password and a personal identification number for protecting the financial card information.

11. The article of manufacture recited in claim 10, wherein the at least one of a password and a personal identification number is encrypted.

12. The article of manufacture recited in claim 1, wherein the server emulation software includes software for establishing a connection between the host device and at least one Internet website and for enabling the consumer to shop on the Internet website for at least one of a product and a service.

13. The article of manufacture recited in claim 12, wherein the server emulation software includes software for providing the financial card information to the Internet website when the consumer obtains at least one of a product and a service.

14. The article of manufacture recited in claim 13, wherein the host device is connected to the Internet website via a dedicated server including software associated with the server emulation software for receiving the financial card information.

15. The article of manufacture recited in claim 13, wherein the dedicated server includes software for decrypting the financial card information.

16. The article of manufacture recited in claim 14, wherein the Internet website includes an application program interface associated with the server emulation software for communicating with the server emulation software.

17. An article of manufacture comprising a computer readable medium on which server emulation software is stored and from which Interactive Media Site (IMS) software can be accessed by a local host device, wherein the computer readable medium comprises:

at least one virtual store from which a consumer may obtain at least one of a product and a service;

financial card information for providing payment for the at least one of the product and the service obtained by the consumer;

a consumer banking identification number for associating the consumer with a cardholder account; and

merchant account information identifying at least one merchant associated with the at least one virtual store.

18. The article of manufacture recited in claim 17, wherein the financial card information comprises at least one of an encrypted credit card number and an encrypted debit card number.

19. The article of manufacture recited in claim 17, wherein the merchant account information comprises a number associated with a merchant's financial card processing account.

20. The article of manufacture recited in claim 17, wherein at least one of the consumer banking identification number and the merchant identification number are encrypted.

21. The article of manufacture recited in claim 17, wherein at least one of the financial card information, the consumer banking identification number and the merchant identification number are embedded on the computer readable medium using an application program interface associated with the server emulation software.

22. The article of manufacture recited in claim 17, wherein at least one of the financial card information, the consumer banking identification number and the merchant identification number are automatically loaded into a memory device of the host device when the computer readable medium is accessed.

23. The article of manufacture recited in claim 22, wherein the memory device is a random access memory device.

24. The article of manufacture recited in claim 22, wherein the memory device is at least one of flushed and overwritten when the consumer completes a transaction.

25. The article of manufacture recited in claim 17, wherein the at least one of the financial card information, the consumer banking identification number and the merchant identification number is relegated to first in first out access in the host device when the computer readable medium is accessed such that a port conveying the financial card information is only opened for a short period of time.

26. The article of manufacture recited in claim 17, wherein at least one of the financial card information, the consumer banking identification number and the merchant identification number is password protected.

27. The article of manufacture recited in claim 26, wherein the consumer pre-registers at least one of a password and a personal identification number with a financial institution that issued the computer readable medium to the consumer.

28. The article of manufacture recited in claim 17, wherein the server emulation software includes software for establishing a direct connection between the host device and a clearing bank.

29. The article of manufacture recited in claim 28, wherein when the consumer obtains at least one of a product and a service from the at least one virtual store, the host device provides directly to the clearing bank at least one of a transaction amount, the financial card information, and the merchant account information.

30. The article of manufacture recited in claim 29, wherein the at least one of a transaction amount, the financial card information, and the merchant account information is provided to the clearing bank via a secure communication protocol.

31. The article of manufacture recited in claim 29, wherein the clearing bank employs an application program interface associated with the server emulation software for receiving the at least one of a transaction amount, the financial card information, and the merchant account information.

32. The article of manufacture recited in claim 31, wherein the application program interface decrypts at least one of the financial card information and the merchant account information received directly from the host device.

33. The article of manufacture recited in claim 28, wherein when the consumer obtains at least one of a product and a service from the at least one virtual store, the host device provides to the merchant associated with the at least one virtual store at least one of a purchase order, the consumer banking identification number and the consumer's name and address.

34. The article of manufacture recited in claim 33, wherein the merchant employs an application program interface associated with the server emulation software to receive the at least one of a purchase order, the consumer banking identification number and the consumer's name and address.

35. The article of manufacture recited in claim 33, wherein the at least one of a purchase order, the consumer banking identification number and the consumer's name and address are provided to the merchant via a network.

36. The article of manufacture recited in claim 33, wherein the at least one of a purchase order, the consumer banking identification number and the consumer's name and address are provided to the merchant via the Internet.

37. The article of manufacture recited in claim 33, wherein the at least one of a purchase order, the consumer banking identification number and the consumer's name and address are provided to the merchant via at least one of e-mail, facsimile, or mail.

38. The article of manufacture recited in claim 33, wherein the application program interface decrypts the consumer banking identification number.

39. The article of manufacture recited in claim 17, wherein the server emulation software includes software for establishing a connection between the host device and a clearing bank via a dedicated server including software associated with the server emulation software for receiving at least one of an amount to be verified, the financial card information, the consumer banking identification number and the merchant account information.

40. The article of manufacture recited in claim 39, wherein when the consumer obtains at least one of a product and a service from the at least one virtual store, the host device provides to the dedicated server at least one of a transaction amount, the financial card information, and the merchant account information.

41. The article of manufacture recited in claim 40, wherein the dedicated server provides to the clearing bank the at least one of a transaction amount, the financial card information, and the merchant account information.

42. The article of manufacture recited in claim 17, wherein the at least one virtual store is accessible to the consumer for a predetermined period of time.

43. The article of manufacture recited in claim 17, wherein the server emulation software includes software for establishing a connection between the host device and at least one Internet website and for enabling the consumer to shop on the Internet website for at least one of a product and a service.

44. The article of manufacture recited in claim 43, wherein the host device is connected to the Internet website via a dedicated server including software associated with the server emulation software for receiving the consumer banking identification number.

45. The article of manufacture recited in claim 44, wherein the Internet website includes an application program interface associated with the server emulation software for communicating with the server emulation software.

46. An article of manufacture comprising a computer readable medium on which server emulation software is stored and from which Interactive Media Site (IMS) software can be accessed by a local host device, wherein the computer readable medium comprises:

an encrypted data string including identity verification information; and

software for decrypting the data string.

47. The article of manufacture recited in claim 46, wherein the server emulation software includes software for establishing a connection between the host device and at least one Internet website and for enabling the consumer to shop on the Internet website for at least one of a product and a service.

48. The article of manufacture recited in claim 46, wherein the data string comprises a randomly generated number and at least one of a password and a personal identification number.

49. The article of manufacture recited in claim 48, wherein the at least one of a password and a personal identification number is provided for identity verification by a consumer to a financial institution that issues the computer readable medium to the consumer.

50. The article of manufacture recited in claim 48, wherein the randomly generated number is generated by the issuing financial institution and associated with a cardholder account.

51. The article of manufacture recited in claim 46, wherein the identity verification information is embedded on the computer readable medium using an application program interface associated with the server emulation software.

52. The article of manufacture recited in claim 46, wherein the software for decrypting the data string includes software for providing an encryption layer.

53. The article of manufacture recited in claim 52, wherein the encryption layer comprises algorithms for encrypting and decrypting the identity verification information.

54. The article of manufacture recited in claim 52, wherein the encryption layer comprises algorithms for disassembling and reassembling the identity verification information.

55. The article of manufacture recited in claim 52, wherein the encryption layer comprises algorithms for re-sequencing the identity verification information.

56. The article of manufacture recited in claim 46, wherein the server emulation software further comprises software for establishing a connection with a financial institution that issued the computer readable medium and for providing to the financial institution the identity verification information.

57. The article of manufacture recited in claim 56, wherein the server emulation software comprises algorithms for disassembling the identity verification information before providing the identity verification information to the financial institution.

58. The article of manufacture recited in claim 56, wherein the server emulation software comprises algorithms for altering the sequence in which the identity verification information is received by the financial institution.

59. The article of manufacture recited in claim 56, wherein the server emulation software establishes the connection with the financial institution via an application program interface associated with the server emulation software.

60. The article of manufacture recited in claim 56, wherein the application program interface comprises algorithms for disassembling and reassembling identity verification information.

61. The article of manufacture recited in claim 56, wherein the application program interface comprises algorithms for sequencing and re-sequencing identity verification information.

62. The article of manufacture recited in claim 46, wherein the server emulation software further comprises software for:

querying a consumer for a first password;

reading the first password entered by the consumer;

accessing the identity verification information on the computer readable medium;

decrypting the identity verification information;

isolating the at least one of a password and a personal identification number; and

comparing the at least one of a password and a personal identification number with the first password entered by the consumer.

63. The article of manufacture recited in claim 62, wherein the server emulation software further comprises software for:

isolating the randomly generated number when the at least one of a password and a personal identification number matches the first password entered by the consumer;

establishing a connection with a financial institution that issued the computer readable medium;

accessing a cardholder account associated with the randomly generated number; and

receiving queries from the financial institution.

64. The article of manufacture recited in claim 63, wherein establishing a connection with the financial institution comprises establishing the connection via an application program interface associated with the server emulation software.

65. The article of manufacture recited in claim 63, wherein accessing a cardholder account comprises accessing a data string associated with the cardholder account.

66. The article of manufacture recited in claim 65, wherein accessing a data string associated with the cardholder account comprises accessing the data string via an application program interface associated with the server emulation software.

67. The article of manufacture recited in claim 66, wherein the application program interface includes software for encrypting and decrypting the data string.

68. The article of manufacture recited in claim 66, wherein the application program interface includes software for assembling and disassembling the data string.

69. The article of manufacture recited in claim 66, wherein the application program interface includes software for sequencing and re-sequencing the data string.

70. The article of manufacture recited in claim 63, wherein receiving queries comprises receiving a request for at least one of an additional password, an additional personal identification number, and a machine identification.

71. The article of manufacture recited in claim 65, wherein the data string comprises a copy of the randomly generated number and the at least one of a password and a personal identification number.

72. The article of manufacture recited in claim 71, wherein the data string further comprises additional identity verification information.

73. The article of manufacture recited in claim 72, wherein the additional identity verification information comprises at least one of an additional password and an additional personal identification number.

74. The article of manufacture recited in claim 72, wherein the additional identity verification information comprises a machine identification.

75. The article of manufacture recited in claim 73, wherein the server emulation software further comprises software for:

querying the consumer for a second password;

reading the second password entered by the consumer;

providing the second password to the financial institution; and

receiving from the financial institution the consumer's financial card information, when the second password matches the at least one of an additional password and an additional personal identification number.

76. The article of manufacture recited in claim 74, wherein the server emulation software further comprises software for:

querying the host device for a machine identification;

reading the machine identification from the host device;

providing the machine identification to the financial institution; and

receiving from the financial institution the consumer's financial card information, when the transmitted machine identification matches the machine identification included in the identity verification information.

77. The article of manufacture recited in claim 75, wherein the financial card information comprises at least one of a financial card number and cardholder account information.

78. The article of manufacture recited in claim 75, wherein the server emulation software further comprises software for providing the financial card information directly to a clearing bank.

79. The article of manufacture recited in claim 75, wherein the server emulation software further comprises software for providing the financial card information directly to a consolidated bank.

80. The article of manufacture recited in claim 75, wherein the server emulation software further comprises software for providing the consumer's name and address to a carrier.

81. The article of manufacture recited in claim 47, wherein the server emulation software further comprises software for providing to a merchant a customer identification number.

82. The article of manufacture recited in claim 56, wherein the server emulation software includes software for establishing a connection with the financial institution via a dedicated server.

83. The article of manufacture recited in claim 82, wherein the dedicated server includes software associated with the server emulation software for disassembling the identity verification information before providing the identity verification information to the financial institution.

84. The article of manufacture recited in claim 82, wherein the dedicated server includes software associated with the server emulation software for altering the sequence in which the identity verification information is received by the financial institution.

85. A method for enabling a consumer to engage in an E-commerce transaction requiring a financial card, the method comprising:

providing to the consumer a computer readable medium on which server emulation software is stored and from which Interactive Media Site (IMS) software can be accessed by a local host device;

providing on the computer readable medium at least one virtual store from which a consumer may obtain at least one of a product and a service; and

providing on the computer readable medium financial card information for providing payment for the at least one of the product and the service obtained by the consumer.

86. The method recited in claim 85, further comprising:

providing on the computer readable medium a consumer banking identification number for associating the consumer with a cardholder account; and

providing on the computer readable medium merchant account information identifying at least one merchant associated with the at least one virtual store.

87. A method for enabling a consumer to engage in an E-commerce transaction requiring a financial card, the method comprising:

providing to the consumer a computer readable medium on which server emulation software is stored and from which Interactive Media Site (IMS) software can be accessed by a local host device;

providing on the computer readable medium an encrypted data string including identity verification information; and

providing on the computer readable medium software for decrypting the data string.

88. The method recited in claim 87, further comprising:

querying the consumer for a first password;

reading the first password entered by the consumer;

accessing the identity verification information on the computer readable medium;

decrypting the identity verification information;

isolating at least one of a password and a personal identification number included in the data string; and

comparing the at least one of a password and a personal identification number with the first password entered by the consumer.

89. The method recited in claim 88, further comprising:

isolating a randomly generated number included in the data string when the at least one of a password and a personal identification number matches the first password;

establishing a connection with a financial institution;

accessing a cardholder account associated with the randomly generated number; and

receiving queries from the financial institution.

90. The method recited in claim 89, wherein receiving queries comprises receiving a request for at least one of an additional password, an additional personal identification number, and a machine identification.

91. The method recited in claim 90, further comprising:

querying the consumer for a second password;

reading the second password entered by the consumer;

providing the second password to the financial institution; and

receiving from the financial institution the consumer's financial card information, when the at least one of an additional password and an additional personal identification number matches the second password.

92. A method for enabling a consumer to engage in an E-commerce transaction requiring a financial card, the method comprising:

receiving from a bank customer identity verification information;

generating a randomly generated number;

combining the randomly generated number and identity verification information into a first data string; and

associating the first data string with a cardholder account maintained for the bank customer by a financial institution.

93. The method recited in claim 92, further comprising:

encrypting the first data string; and

storing the first data string in a customer records data base.

94. The method recited in claim 93, wherein the identity verification information comprises at least one of a password and a personal identification number.

95. The method recited in claim 93, wherein the identity verification information comprises a merchant identification.

96. The method recited in claim 93, further comprising:

combining a copy of the randomly generated number and a copy of a portion of the identity verification information into a second data string;

embedding the second data string on a computer readable medium;

providing the computer readable medium to the bank customer.

97. The method recited in claim 96, wherein the a portion of the identity verification information comprises at least one of a password and a personal identification number.

98. The method recited in claim 96, further comprising encrypting the second data string.

99. The method recited in claim 96, wherein providing the computer readable medium to the bank customer comprises sending the computer readable medium to the bank customer by mail.

100. The method recited in claim 96, further comprising providing on the computer readable medium server emulation software from which Interactive Media Site (IMS) software can be accessed by a local host device.

101. The method recited in claim 100, wherein the server emulation software includes software for:

querying the bank customer for a first password;

reading the first password entered by the bank customer;

accessing the identity verification information on the computer readable medium;

decrypting the identity verification information on the computer readable medium;

isolating at least one of a password and a personal identification number included in the second data string; and

comparing the at least one of a password and a personal identification number with the first password entered by the bank customer.

102. The method recited in claim 101, wherein the server emulation software further includes software for:

isolating the copy of the randomly generated number in the second data string when the at least one of a password and a personal identification number matches the first password;

establishing a connection with the financial institution;

accessing the cardholder account associated with the randomly generated number; and

receiving queries from the financial institution.

103. The method recited in claim 102, wherein receiving queries comprises receiving a request for at least one of an additional password, an additional personal identification number, and a machine identification.

104. The method recited in claim 103, wherein the server emulation software further includes software for:

querying the consumer for a second password;

reading the second password entered by the consumer;

providing the second password to the financial institution; and

receiving from the financial institution the consumer's financial card information, when the at least one of an additional password and an additional personal identification number matches the second password.